09/46[redacted]15 S99P0494 WO00
PCT/JP99/02404
REC'D 21 MAY 1999 10.05.99
WIPO PCT
EKJ

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

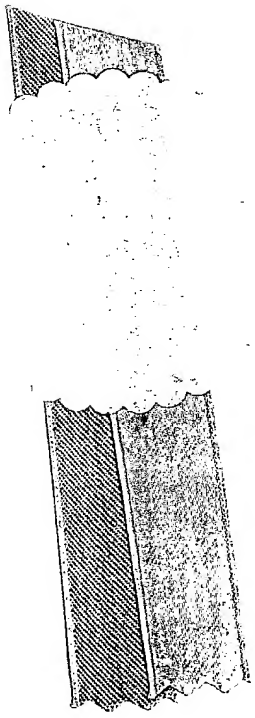
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　５月１１日

出願番号
Application Number: 平成１０年特許願第１２７２２７号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



１９９９年　３月２６日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号　出証特平１１－３０１９３８２

【書類名】　特許願
【整理番号】　9800055702
【提出日】　平成10年 5月11日
【あて先】　特許庁長官　荒井　寿光　殿
【国際特許分類】　H04L 12/00
【発明の名称】　情報配信システム
【請求項の数】　7
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　勝又　泰
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　大林　正之
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　中津山　孝
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　韓　敏哉
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100082762

【弁理士】

【氏名又は名称】　杉浦　正知

【電話番号】　03-3980-0339

【手数料の表示】

【予納台帳番号】　043812

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000002185
【住所又は居所】　東京都品川区北品川６丁目７番３５号
【氏名又は名称】　ソニー株式会社
【代理人】　申請人
【識別番号】　100082762
【住所又は居所】　東京都豊島区東池袋１－４８－１０　２５山京ビル４２０号　杉浦特許事務所
【氏名又は名称】　杉浦　正知

【書類名】　明細書

【発明の名称】　情報配信システム

【特許請求の範囲】

【請求項１】　複数のデータが蓄積されるとともに上記複数のデータの各々に相対する固有情報が蓄積される第１の記憶手段と、

上記複数のデータのうち所定のデータに相対する上記固有情報を用いて上記所定のデータを暗号化する暗号化手段と、

暗号化された上記所定のデータ及び上記所定のデータに相対する固有情報を送信する送信手段と、

を有する情報センタと、

上記送信手段により送信された上記暗号化された所定のデータ及び上記所定のデータに相対する固有情報を受信する受信手段と、

少なくとも上記受信された上記固有情報を蓄積する第２の記憶手段と、

上記暗号化された所定のデータに相対する固有情報により復号化する復号化手段と、

上記受信手段により受信された上固有情報を上記第２の記憶手段に予め記憶された他の上記固有情報と比較する比較手段と、

上記比較手段の判別に応じて課金処理を行う課金処理手段とを有する端末装置と

を備える情報配信システム。

【請求項２】　上記比較手段により、上記受信手段により受信された上記固有情報が上記第２の記憶媒体により予め記憶されていると判断されるとき、上記課金処理手段による課金処理を禁止するようにした請求項１に記載の情報配信システム。

【請求項３】　上記受信手段による受信された上記固有情報に応じて上記課金処理の金額を決定するようにした請求項１に記載の情報配信システム。

【請求項４】　ユーザが有するユーザ固有情報が上記端末装置から上記情報センタに送信され、上記情報センタにおいて上記暗号化された所定のデータ及び上記所定のデータに相対する固有情報を各々上記ユーザ固有情報に暗号化されて

【書類名】　要約書

【要約】

【課題】　コンテンツの配信を行なうようなシステムで、コンテンツの保護が十分図れ、正当な課金が行なえるようにする。

【解決手段】　コンテンツサーバ１０１には、Ｃキーにより暗号化されたコンテンツと、Ｃキーとが蓄積されるコンテンツデータベース１１１を設ける。このＣキーにより暗号化されたコンテンツと、Ｃキーを、Ｍキーで暗号化して、ユーザマシン１０２に送る。ユーザマシン１０２では、Ｃキーにより暗号化されたコンテンツと、Ｃキーをストレージデバイス１２０に保存する。再生時にストレージデバイス１２０からのＣキーにより暗号化されたコンテンツと、Ｃキーを、暗号化／復号化処理チップ１２１に送り、復号すると共に、Ｃキーに応じて、課金を行う。また、Ｃキーに、時間と共に動的に変化するＤＡコードを付加する。このようなＤＡコードを付加することで、Ｃキーを退避させておいて、コンテンツを不正利用するようなことが防止できると共に、ＤＡコードを利用して、コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借するようなことが行なえる。

【選択図】　図３

上記端末装置に送信され、端末装置においてユーザ固有情報により復号化されるようにした請求項１に記載の情報配信システム。

【請求項５】　複数のデータが蓄積されるとともに上記複数のデータの各々に相対する固有情報が蓄積される第１の記憶手段と、

上記複数のデータのうち所定のデータに相対する上記固有情報を用いて上記所定のデータを暗号化する暗号化手段と、

暗号化された上記所定のデータ及び上記所定のデータに相対する固有情報を送信する送信手段と、

を有する情報センタと、

上記送信手段により送信された上記暗号化された所定のデータ及び上記所定のデータに相対する固有情報を受信する受信手段と、

少なくとも上記受信された上記固有情報を蓄積する第２の記憶手段と、

上記暗号化された所定のデータに相対する固有情報により復号化する復号化手段と

を有する端末装置とからなり、

上記固有情報に、更に、時間と共に変化していく時間変化情報を付加し、上記第２の記憶手段に記憶されている上記固有情報を所定時間毎に呼び出し、呼び出された上記固有情報が正しいか否かを判断し、上記呼び出された上記固有情報が正しければ上記固有情報を更新して上記第２の記憶手段に戻し、上記呼び出された上記固有情報が正しくなければ上記所定のデータを利用禁止とする

ようにした情報配信システム。

【請求項６】　上記所定のデータに利用禁止を示す情報を付加して上記所定のデータを利用禁止とするようにした請求項５に記載の情報配信システム。

【請求項７】　上記所定のデータに対する上記固有情報を消去して上記所定のデータを利用禁止とするようにした請求項５に記載の情報配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えば、複数の音楽データが蓄積されるコンテンツサーバと、こ

のコンテンツサーバに蓄積されたコンテンツから所望のコンテンツが配信されるユーザマシンとからなる情報配信システムに関するもので、特に、コンテンツの保護と課金に係わる。

【０００２】

【従来の技術】

近年、インターネットや衛星通信の普及により、コンピュータネットワーク網を利用した種々のサービスが実現されつつある。そのようなコンピュータネットワーク網を使ったサービスのひとつとして、以下のような音楽配信サービスを行なうシステムが提案されている。

【０００３】

図１４において、５０１はコンテンツサーバ、５０２はユーザマシンである。コンテンツサーバ５０１には、複数の音楽データがコンテンツとして蓄積されている。ユーザマシン５０２には、ハードディスクドライブやＭＤドライブ等のストレージデバイス５０４が接続されると共に、課金を行なうためのカードリーダ／ライタ５０５が接続される。カードリーダ／ライタ５０５には、カード５０６が装着される。

【０００４】

音楽配信サービスを利用する場合には、ユーザマシン５０２が伝送路５０３を介してコンテンツサーバ５０１に接続される。伝送路５０３は、例えば、インターネットのようなコンピュータネットワーク網である。３ユーザマシン５０２がコンテンツサーバ１に接続されると、コンテンツサーバ５０１からユーザマシン５０２にコンテンツのリストや検索画面が送られる。

【０００５】

ユーザは、このコンテンツのリストや検索画面で所望のコンテンツを検索して、ダウンロードしたいコンテンツを選択する。ユーザがコンテンツを選択すると、ユーザマシン５０２からコンテンツサーバ５０１にそのコンテンツの要求命令が送られる。コンテンツサーバ５０１で、要求命令に応じてコンテンツが取り出され、このコンテンツがコンテンツサーバ５０１からユーザマシン５０２に送られる。そして、このコンテンツがユーザマシン５０２のストレージデバイス５０

４に保存される。このとき、カードリーダ／ライタ５０５により、適切な課金が行なわれる。

【０００６】

【発明が解決しようとする課題】

このような音楽配信システムが普及すると、ユーザは、所望の楽曲の音楽データを通信で簡単に入手することができる。また、このようなシステムにおけるサーバには、検索機能が備えられており、このような検索機能を使うと、所望の楽曲を検索して、入手することが簡単にできる。更に、このようなシステムにおけるサーバでは、常に音楽データの更新が行われるため、最新の楽曲をいち早く入手することができる。

【０００７】

ところが、このようにサーバからの音楽データをユーザマシンに配信するようなシステムでは、コンテンツのデータが無断で複製され、著作者の権利が守られなくなる危険性がある。このため、コンテンツのデータが無断で複製されることがないように、複製防止のための機能を付加する必要があると共に、コンテンツに対して適切な課金が行なわれる必要がある。

【０００８】

また、このようなシステムでは、ダウンロードした音楽データを他の機器で再生させたり、他人譲渡したりするようなことが考えられる。常に、１台の機器にのみコンテンツのデータが移動されるようにすれば、不正コピーが出回る可能性はない。ところが、他の機器への複製を一切禁止してしまうと、このようなコンテンツのデータの移動も行なえなくなってしまう。

【０００９】

したがって、この発明の目的は、コンテンツの配信を行なうようなシステムで、コンテンツの保護が十分図れ、正当な課金が行なえるようにした情報配信システムを提供することにある。

【００１０】

【課題を解決するための手段】

この発明は、複数のデータが蓄積されるとともに複数のデータの各々に相対す

る固有情報が蓄積される第１の記憶手段と、

複数のデータのうち所定のデータに相対する固有情報を用いて所定のデータを暗号化する暗号化手段と、

暗号化された所定のデータ及び所定のデータに相対する固有情報を送信する送信手段と、

を有する情報センタと、

送信手段により送信された暗号化された所定のデータ及び所定のデータに相対する固有情報を受信する受信手段と、

少なくとも受信された固有情報を蓄積する第２の記憶手段と、

暗号化された所定のデータに相対する固有情報により復号化する復号化手段と、

受信手段により受信された固有情報を第２の記憶手段に予め記憶された他の固有情報と比較する比較手段と、

比較手段の判別に応じて課金処理を行う課金処理手段とを有する端末装置とを備える情報配信システムである。

【００１１】

この発明は、複数のデータが蓄積されるとともに複数のデータの各々に相対する固有情報が蓄積される第１の記憶手段と、

複数のデータのうち所定のデータに相対する固有情報を用いて所定のデータを暗号化する暗号化手段と、

暗号化された所定のデータ及び所定のデータに相対する固有情報を送信する送信手段と、

を有する情報センタと、

送信手段により送信された暗号化された所定のデータ及び所定のデータに相対する固有情報を受信する受信手段と、

少なくとも受信された固有情報を蓄積する第２の記憶手段と、

暗号化された所定のデータに相対する固有情報により復号化する復号化手段とを有する端末装置とからなり、

固有情報に、更に、時間と共に変化していく時間変化情報を付加し、第２の記

憶手段に記憶されている固有情報を所定時間毎に呼び出し、呼び出された固有情報が正しいか否かを判断し、呼び出された固有情報が正しければ固有情報を更新して第２の記憶手段に戻し、呼び出された固有情報が正しくなければ所定のデータを利用禁止とする

ようにした情報配信システムである。

【００１２】

コンテンツサーバに保存されるコンテンツは、Ｃキーで暗号化されている。このように、Ｃキーを設けることにより、コンテンツを移動したり、譲渡したり、再送を要求したりできる。また、送られてきたＣキーと同一のＣキーがストレージに保存されているか否かを判断することにより、再送か否かを判断して、適切な課金を行なったり、Ｃキーにランクを付けてコンテンツ毎に料金を変えて課金を行なうようなことができる。

【００１３】

また、Ｃキーに、時間と共に動的に変化するＤＡコードが付加される。このようなＤＡコードを付加することで、Ｃキーを退避させておいて、コンテンツを不正利用するようなことが防止できる。また、この時間と共に動的に変化するＤＡコードを利用して、コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借するようなことが行なえる。

【００１４】

【発明の実施の形態】

以下、この発明の実施の形態について図面を参照して説明する。この発明は、コンテンツのデータを転送するようなシステムにおいて、コンテンツのデータの保護が図れると共に、適切な課金が行なえるようにしたものである。このようなシステムにで用いられる暗号化キーやコードについて先ず簡単に説明しておく。

【００１５】

１．キー及びコードの説明

この発明が適用されたシステムでは、以下のような暗号化キーやコードが用いられる。

【００１６】

（１）Ｍキー

Ｍ（Machine ）キーの役割は、特定の機器でのみデータを利用可能とすることである。Ｍキーは例えば機器の工場出荷時に各機器毎に与えられるもので、各機器固有の暗号化情報である。Ｍキーは、保護を図るために、例えば機器の暗号化／復号化処理チップ内に埋め込まれ、機器内から外へは取り出せないようになっている。

【００１７】

（２）ＭＩＤコード

各機器には、固有のＭＩＤ（Machine Idnetification）コードが付与される。このＭＩＤコードも、工場出荷時に各機器に付与される。ＭＩＤコードは、各機器を特定するためにのみ使用されるものであり、直接的に暗号化キーとして用いられるものではない。したがって、外部に漏れても、データの保護が守られなくなる危険性は少ない。ＭＩＤコードは、Ｍキーと同様に、例えば機器の暗号化／復号化処理チップ内に埋め込んでおいても良いし、別のＲＯＭやＥＥＰＲＯＭに蓄えておいても良い。

【００１８】

（３）Ｃキー

Ｃ（Contents）キーの役割は、各コンテンツ毎にデータの保護を図ることである。ここで、コンテンツとは、移転できる１かたまりの情報の単位とする。すなわち、データを課金するようなシステムでは、１つの課金の対象となる情報の単位である。音楽サーバのような場合には、１曲毎に課金をするとすると、各曲の音楽データという単位が１つのコンテンツのデータとなる。

【００１９】

各コンテンツは、各コンテンツに固有のＣキーを用いて暗号化される。したがって、そのコンテンツに対応するＣキーを有しているユーザ側の機器でのみ、そのＣキーを使ってコンテンツの暗号を解読して、再生することが可能である。このように、Ｃキーを有しているユーザ側の機器でのみ、そのコンテンツを利用可能なことから、Ｃキーは、そのコンテンツを利用できる権利を表すキーという見

方もできる。

【００２０】

（４）Ｔキー

Ｔ（Transfer）キーの役割は、各ユーザ機器間でデータの移動を行う際に、データの保護を図るためのものである。各機器間でコンテンツの移動を行うような場合に、Ｃキーが外部に漏れる可能性がある。このため、各機器間でデータの移動を行う場合には、Ｃキーと、Ｃキーで暗号化されたコンテンツは、更に、Ｔキーで暗号化される。

【００２１】

Ｔキーは、データの受け取り側の機器と、データの送り側の機器との間で予め決められたアルゴリズムで、ＭＩＤコードに基づいて生成される。すなわち、機器間でコンテンツのデータの転送を行う場合には、受け取り側の機器から送り側の機器に対して、受け取り側のＭＩＤコードが送られる。送り側の機器では、送られてきたＭＩＤコードに基づいて、Ｔキーが生成される。また、受け取り側の機器では、自分のＭＩＤに基づいて、同様のアルゴリズムによりＴキーが生成される。

【００２２】

（５）ＤＡコード

暗号／復号化チップ内で生成される動的認証コードであり、Ｃキーに付加される。ＤＡコードは、例えば、乱数、タイムコード等を利用して生成される。このようなＤＡコードを付加しておくと、Ｃキーを一時的に退避させてコンテンツを不正使用することができなくなる。また、ＤＡコードを利用して、所定の期間使用を許可／禁止したり、コンテンツを貸し借りしたりすることができるようになる。

【００２３】

２．Ｍキーを使ったシステムについて

図１は、この発明が適用されたデータ配信システムの一例を示すものである。この例は、Ｍキーと呼ばれる暗号化キーを導入して、特定の機器でのみデータを利用可能にするようにしたものである。

【００２４】

図１において、１はコンテンツサーバ、２はユーザマシン、３はコンテツサーバ１とユーザマシン２とを結ぶ伝送路である。コンテンツサーバ１には、コンテンツデータベース１１が設けられる。このコンテンツデータベース１１には、コンテンツサーバ１で提供するコンテンツのデータが格納されている。

【００２５】

コンテンツデータベータ１１に格納されるコンテンツのデータは、コンテンツ入力端子１３から与えられる。例えば、音楽配信サービスを行なうサーバの場合には、コンテンツ入力端子１３から音楽データが与えられる。この音楽データは、エンコーダ１４に供給される。エンコーダ１４で、この音楽データが例えばＡＴＲＡＣ（Adaptive Transform Acoustic Coding）で圧縮符号化される。この圧縮された音楽データがコンテンツデータベース１１に蓄えられる。

【００２６】

また、コンテンツサーバ１には、コード及びキーデータベース１２が設けられる。このコード及びキーデータベース１２には、コンテンツサーバ１に繋がれる全ての機器のユーザマシン２のＭＩＤコードとＭキーとが蓄えられる。ＭＩＤコードは、各ユーザマシン２を識別するためのユーザマシン毎の固有の情報である。Ｍキーは、各ユーザマシン毎に固有の暗号化キーである。ＭＩＤコード及びＭキーは例えば機器の工場出荷時に各ユーザマシン２に与えられる。ＭＩＤコード及びＭキーを工場出荷時に各ユーザマシン２に付与する際に、各機器毎に付与したＭＩＤコード及びＭキーのリストに基づいてコード及びキーデータベータ１２が作成される。

【００２７】

コンテンツサーバ１の全体動作は、サーバ処理マネージャ１６により管理されている。また、コンテンツサーバ１の通信制御は、通信マネージャ１５により管理されている。コンテンツサーバ１からのデータは、暗号化回路１７により暗号化される。このときの暗号化は、ユーザマシン２から送られてきたＭＩＤコードに基づいてコード及びキーデータベース１２で検索されたＭキーにより行なわれる。

【００２８】

一方、ユーザマシン２には、暗号化／復号化処理チップ２１が設けられる。この暗号化／復号化処理チップ２１は、データの暗号化処理及び暗号の復号化処理を行う専用のチップである。この暗号化／復号化処理チップ２１には、工場出荷時に、機器固有のＭＩＤコードと、Ｍキーが格納されている。

【００２９】

図２は、暗号化／復号化処理チップ２１の構成を示すものである。暗号化／復号化処理チップ２１には、Ｍキーホルダ５１と、ＭＩＤコードホルダ５２と、Ｍキー復号化回路５３と、コントローラ５４が設けられる。Ｍキーホルダ５１には、各機器固有の暗号化情報であるＭキーが工場出荷時に記憶される。ＭＩＤコードホルダ５２には、各機器固有の識別情報であるＭＩＤコードが工場出荷時に記憶される。コントローラ５４は、暗号化／復号化処理チップ２１の動作を制御している。

【００３０】

コントローラ５４には、コマンド端子ＣＭＤからコマンドが与えられる。このコマンドに基づいて、暗号化／復号化処理チップ２１の動作が設定される。Ｍキー復号化回路５３には、入力端子ＤＡＴＡ＿ＩＮからＭキーで暗号化されたデータが供給される。また、Ｍキー復号化回路５３には、Ｍキーホルダ５１からＭキーが供給される。Ｍキー復号化回路５３で、入力データの暗号解読を行なわれる。Ｍキー復号回路５３の出力は、データ出力端子ＤＡＴＡ＿ＯＵＴから出力される。また、ＭＩＤコードホルダ５２からは、コード出力端子ＭＩＤ＿ＯＵＴが導出される。このコード出力端子ＭＩＤ＿ＯＵＴからは、ＭＩＤコードが出力される。

【００３１】

図２に示すように、暗号化／復号化の処理は、１チップの暗号化／復号化処理チップ２１で行われ、この暗号化／復号化処理チップ２１内に、Ｍキーと、ＭＩＤコードが格納されている。このため、外部からは、暗号処理がどのようにして行われ、暗号化キーが何であるのかは解明できない。

いる。通信マネージャ１５がユーザマシン２からの配信要求、ＭＩＤコード、課金情報を受信すると、これら情報は、サーバ処理マネージャ１６に送られる。

【００３７】

サーバ処理マネージャ１６は、ユーザマシン２からＭＩＤコードを受信したら、このＭＩＤコードをコード及びキーデータベース１２に送り、そのＭＩＤコードに対応する機器のＭキーを問い合わせる。コード及びキーデータベース１２は、各機器毎のＭＩＤコードと、これに対応するＭキーの情報が予め格納されている。コード及びキーデータベース１２は、ＭＩＤコードを受け付けると、このＭＩＤコードから機器を識別し、この機器に対応するＭキーを出力する。このＭキーは、Ｍキー暗号化回路１７に送られる。これにより、Ｍキー暗号化回路１７に、暗号化キーがセットされる。

【００３８】

また、サーバ処理マネージャ１６は、ユーザマシン２からの配信要求を受け付けると、要求されたコンテンツの配信指示をコンテンツデータベース１１に送る。コンテンツデータベース１１は、配信指示を受け取ると、要求されたコンテンツのデータの読み出しを行なう。読み出されたコンテンツのデータは、Ｍキー暗号化回路１７に送られる。

【００３９】

Ｍキー暗号化回路１７には、コード及びキーデータベース１２から、データを要求したユーザマシン２の機器のＭＩＤコードに対応したＭキーがセットされている。コンテンツデータベース１１から送られるコンテンツのデータは、Ｍキー暗号化回路１７で、このＭキーにより暗号化される。そして、このＭキーで暗号化されたコンテンツのデータは、コンテンツサーバ１の通信マネージャ１５から、通信路３を介して、ユーザマシン２の通信路マネージャ２５に送られる。そして、このコンテンツのデータは、ユーザマシン２にあるストレージデバイス２０に蓄積される。

【００４０】

このように、ユーザマシン２からコンテンツサーバ１にコンテンツのダウンロードを要求する際に、ユーザマシン２からコンテンツサーバ１に、その機器固有

【００３２】

図１において、ユーザマシン２には、入力部２２から入力が与えられる。入力部２２からの入力は、ユーザインターフェース２３を介して、マシン処理マネージャ２４に与えられる。

【００３３】

マシン処理マネージャ２４は、ユーザマシン２の全体処理を行っている。マシン処理マネージャ２４は、入力部２２からコンテンツサーバ１のコンテンツを獲得すべき入力を受け付けると、暗号化／復号化処理チップ２１にコマンドを与え、ＭＩＤコードを問い合わせる。暗号化／復号化処理チップ２１は、このようなコマンドを受け付けると、このコマンドに対応して、ＭＩＤコードホルダ５２（図２）に記憶されているＭＩＤコードを出力する。

【００３４】

マシン処理マネージャ２４は、暗号化／復号化処理チップ２１からＭＩＤコードを受け取ったら、通信マネージャ２５に、配信要求と、ＭＩＤコードと、課金情報を送る。これら配信要求、ＭＩＤコード、課金情報は、通信処理マネージャ２５から、通信路３を介して、コンテンツサーバ１の通信マネージャ１５に送られる。

【００３５】

なお、コンテンツサーバ１からのコンテンツの配信サービスを受ける場合には、カード２６が装着される。そして、このカード２６の残高情報がカードリーダ／ライタ２７を介してマシン処理マネージャ２４に送られる。そして、コンテンツの配信が実行されると、マシン処理マネージャ２４は、カードリーダ／ライタ２７を介して、カード２６に、引き出し指示を与え、カード２６から、コンテンツの代金が差し引かれる。このようにして、コンテンツに対する代金の支払いが行なわれる。このとき、正規のユーザか否か、ユーザが確かに課金を行っているか否かをチェックしてから、ＭＩＤコードに対応するＭキーを出力させるようにしても良い。

【００３６】

コンテンツサーバ１側では、サーバ処理マネージャ１６が全体処理を行なって

のＭＩＤコードが送られる。コンテンツサーバ１には、コード及びキーデータベース１２が設けられており、このコード及びキーデータベース１２により、ユーザマシン２から送られてきた機器のＭＩＤコードに対応するＭキーが呼び出され、コンテンツのデータがこのＭキーで暗号化される。そして、機器固有のＭキーで暗号化されたコンテンツのデータがユーザマシン２に送られ、ユーザマシン２のストレージデバイス２０に蓄えられる。ストレージデバイス２０に蓄えられたコンテンツのデータは、機器固有のＭキーで暗号化されているので、コンテンツの配信を要求したユーザマシン２以外では復号が行なえない。これにより、コンテンツの著作権を守ることができる。

【００４１】

すなわち、ストレージデバイス２０に蓄えられたコンテンツのデータを復号する場合には、そのデータは、ストレージデバイス２０から、図２における暗号化／復号化処理チップ２１のデータ入力端子ＤＡＴＡ＿ＩＮに送られる。図２に示したように、暗号化／復号化処理チップ２１のＭキーホルダ５１には、その機器固有のＭキーが蓄えられている。コンテンツサーバ１から送られてきたコンテンツのデータは、ＭＩＤコードホルダ５２のＭＩＤコードに対応するＭキーで暗号化されているため、コンテンツサーバ１側のＭキー暗号化回路１７に設定されたＭキーは、Ｍキーホルダ５１に格納されているＭキーと同様である。したがって、ストレージ２０からのＭキーで暗号化されたコンテンツのデータは、暗号化／復号化処理チップ２１で、復号することができる。

【００４２】

これに対して、ストレージデバイス２０に蓄えられていたコンテンツのデータを、ユーザマシン２以外の機器に複製したとする。ストレージデバイス２０に蓄えられていたコンテンツのデータは、この機器固有のＭキーで暗号化されている。他の機器の暗号化／復号化処理チップ２１は、この機器と同様のＭキーを有していない。このため、ストレージデバイス２０に蓄えられていたコンテンツのデータをユーザマシン２以外の機器に複製したとしても、その機器では、コンテンツのデータの暗号を解読できない。

【００４３】

３．Ｃキーを使ったシステムについて

上述のように、Ｍキーを導入することで、特定の機器でのみコンテンツのデータが利用可能となる。ところが、Ｍキーだけでは、その機器からコンテンツのデータを移動させることが一切できなくなってしまう。コンテンツのデータが限りなく複製されてしまうと著作者の権利が守られなくなることが考えられるが、コンテンツのデータが移動されただけなら、コンテンツのデータを利用する機器が移っただけなので、問題は生じない。Ｍキーだけでは、このようなコンテンツのデータの移動に対応できない。また、ユーザマシンに一度蓄積しておいたコンテンツのデータがエラーになってしまったり、ダウンロードに失敗したりするようなことが考えられる。このような場合、正規のユーザが正当な課金をしてそのコンテンツのデータの配信を受けているなら、再度、そのコンテンツのデータを配信し直すことが望まれる。また、コンテンツには有料のコンテンツと無料のコンテンツがあり、Ｍキーのみでは、コンテンツの種類に応じて適切な課金が行なえない。

【００４４】

このように、Ｍキーを導入することで、各機器を単位とするデータの保護は図れるが、Ｍキーだけでは、各コンテンツ毎のデータの保護を図り、適切な課金を行なうには不十分である。そこで、コンテンツ毎の暗号化を行うＣキーが導入される。

【００４５】

図３は、Ｃキーを導入したシステムの一例を示すものである。Ｃキーの役割は、各コンテンツ毎にデータの保護を図ることである。

【００４６】

Ｃキーを導入したシステムにおいては、ユーザマシン１０２側の暗号化／復号化処理チップ１２１として、図４に示すように、Ｍキーホルダ１５１と、ＭＩＤコードホルダ１５２と、Ｍキー復号化回路１５３と、コントローラ１５４とが設けられると共に、更に、Ｃキー取り込み回路１５５と、Ｃキー復号化回路１５６とが設けられる。Ｍキーホルダ１５１、ＭＩＤコードホルダ１５２、Ｍキー復号

化回路１５３、コントローラ１５４の動作は、前述のＭキーのみのシステムにおける暗号化／復号化処理チップ２１と同様であり、Ｍキーホルダ１５１には、各機器固有の暗号化情報であるＭキーが工場出荷時に記憶され、ＭＩＤコードホルダ１５２には、各機器固有の識別情報であるＭＩＤコードが工場出荷時に記憶され、コントローラ１５４は、暗号化／復号化処理チップ１２１の動作を制御している。Ｃキー取り込み回路１５５は、Ｍキーの解読により復号されたＣキーを保持するものである。Ｃキー復号回路１５６は、Ｃキーによる復号化処理を行なうものである。

【００４７】

コントローラ１５４には、コマンド端子ＣＭＤからコマンドが与えられ、このコマンドに基づいて、暗号化／復号化処理チップ１２１の動作が設定される。Ｍキー復号化回路１５３には、入力端子ＤＡＴＡ＿ＩＮから、Ｃキーで暗号化され更にＭキーで暗号化されたデータと、入力端子ＫＥＹ＿ＩＮからのＭキーで暗号化されたＣキーが供給される。また、Ｍキー復号化回路１５３には、Ｍキーホルダ５１からＭキーが供給される。

【００４８】

入力データの暗号化キーがＭキーホルダ１５１からのＭキーと一致していれば、Ｍキー復号化回路１５３で、暗号解読を行なえる。Ｍキー復号化回路１５３からは、Ｃキーと、Ｃキーで暗号化されたデータが得られる。このＣキーがＣキー取り込み回路１５５に保持される。また、Ｃキーで暗号化されたデータがＣキー復号化回路１５６に供給される。

【００４９】

Ｃキー復号化回路１５６で、Ｃキーの復号が行なわれ、データが解読される。このＣキー復号回路１５６の出力は、データ出力端子ＤＡＴＡ＿ＯＵＴから出力される。また、ＭＩＤコードホルダ１５２からは、コード出力端子ＭＩＤ＿ＯＵＴが導出される。このコード出力端子ＭＩＤ＿ＯＵＴからは、ＭＩＤコードが出力される。また、Ｃキーで暗号化されてデータを転送するために、Ｃキーの出力端子ＫＥＹ＿ＯＵＴと、Ｃキーで暗号化されたデータの出力端子ＤＡＴＡ＿Ｔが設けられる。

【００５０】

このように、Ｃキーを導入したシステムにおいては、図３におけるユーザマシン１０２側の暗号化／復号化処理チップ１２１として、図４に示すような構成のものが用いられる。また、図３に示すように、コンテンツサーバ１０１側には、Ｃキーを発生するＣキー生成部１１８と、このＣキーを使って、コンテンツのデータを暗号化するＣキー暗号化回路１１９が設けられる。それ以外の構成については、前述の図１に示したＭキーだけの例と同様である。

【００５１】

前述のＭキーだけのシステム例では、コンテンツ入力端子１３からのデータは、エンコーダ１４で圧縮符号化されて、そのままコンテンツデータベース１１に蓄積されたが、この例では、コンテンツ入力端子１１３からのデータは、エンコーダ１１４で圧縮符号化された後、Ｃキー暗号化回路１１９に送られ、Ｃキー生成部１１８からのＣキーにより暗号化されて、コンテンツデータベース１１１に蓄積される。そして、このときのＣキーがコンテンツデータベース１１１に蓄積される。

【００５２】

ユーザマシン１０２のユーザがコンテンツサーバ１０１のコンテンツの配信を受けたい場合には、入力部１２２からユーザインターフェース１２３を介して、マシン処理マネージャ１２４に入力が与えられる。

【００５３】

マシン処理マネージャ１２４は、コンテンツサーバ１０１のコンテンツを獲得すべき入力を受け付けると、暗号化／復号化処理チップ１２１にコマンドを与え、ＭＩＤコードを問い合わせる。暗号化／復号化処理チップ１２１は、暗号化／復号化処理チップ１２１からコマンドが与えられると、このコマンドに対応して、ＭＩＤコードを出力する。

【００５４】

マシン処理マネージャ１２４は、ＭＩＤコードを受け取ったら、通信マネージャ１２５に、配信要求と、ＭＩＤコードと、課金情報を送る。これらの情報は、通信処理マネージャ１２５から、通信路１０３を介して、コンテンツサーバ１０

１の通信マネージャ１１５に送られる。

【００５５】

通信マネージャ１１５は、ユーザマシン１０２からのＭＩＤコードを受け取ったら、このＭＩＤコードをサーバマネージャ１１６に送る。サーバマネージャ１１６は、コード及びキーデータベース１１２にこのＭＩＤコードを送り、そのＭＩＤコードに対応するＭキーを問い合わせる。コード及びキーデータベース１１２は、このＭＩＤコードに対応する機器のＭキーを出力する。コード及びキーデータベース１１２からのＭキーは、Ｍキー暗号化回路１１７に送られ、Ｍキー暗号化回路１１７にＭキーがセットされる。

【００５６】

また、サーバ処理マネージャ１１６は、ユーザマシン１０２からの配信要求を受け付けると、要求されたコンテンツの配信指示をコンテンツデータベース１１１に送る。コンテンツデータベース１１１は、サーバ処理マネージャ１１６からの情報に基づいて、要求されたコンテンツのデータを読み出す。

【００５７】

前述したように、コンテンツデータベース１１１のデータは、Ｃキーにより暗号化されている。したがって、Ｃキーにより暗号化されたコンテンツデータが、更に、Ｍキー暗号化回路１１７により、Ｍキーで暗号化される。また、このときのＣキーがコンテンツデータベース１１１から読み出され、Ｍキー暗号化回路１１７により、Ｍキーにより暗号化される。

【００５８】

このように、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータと、Ｍキーで暗号化されたＣキーは、コンテンツサーバ１０１の通信マネージャ１１５から、通信路１０３を介して、ユーザマシン１０２の通信路マネージャ１２５に送られる。そして、このＣキーで暗号化され更にＭキーで暗号化されたコンテンツのデータと、Ｍキーで暗号化されたＣキーは、ストレージデバイス１２０に蓄積される。

【００５９】

このように、コンテンツデータベース１１１に蓄えられているコンテンツのデ

ータはＣキーで暗号化されており、コンテンツサーバ１０１からユーザマシン１０２にデータが送られる際に、更に、このデータは、Ｍキーで暗号化される。したがって、ストレージデバイス１２０に蓄積されるデータは、Ｃキーで暗号化され、更に、Ｍキーで暗号化されている。Ｃキーで暗号化されたコンテンツのデータを解読するためには、Ｃキーが必要であるが、このＣキーは、コンテンツサーバ１から、Ｍキーで暗号化されて渡されている。

【００６０】

ストレージデバイス１２０に蓄えられたコンテンツのデータを復号する場合には、そのデータは、ストレージデバイス１２０から、図４における暗号化／復号化処理チップ１２１のデータ入力端子ＤＡＴＡ＿ＩＮに送られる。また、Ｍキーで暗号化されたＣキーが、ストレージデバイス１２０から、暗号化／復号化処理チップ１２１のキー入力端子ＫＥＹ＿ＩＮに送られる。

【００６１】

図４に示すように、暗号化／復号化処理チップ１２１のＭキーホルダ１５１には、その機器固有のＭキーが蓄えられている。コンテンツサーバ１０１から送られてきたコンテンツのデータは、ＭＩＤコードホルダ１５２のＭＩＤコードに対応するＭキーで暗号化されているため、コンテンツサーバ１０１側のＭキー暗号化回路１１７に設定されたＭキーは、Ｍキーホルダ１５１に格納されているＭキーと同様である。したがって、ストレージデバイス１２０からの、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータは、Ｍキーについては、Ｍキー復号化回路１５３で、復号することができる。

【００６２】

また、ストレージデバイス１２０からのＭキーで暗号化されたＣキーは、Ｍキー復号化回路１５３で復号される。

【００６３】

したがって、Ｍキー復号化回路１５３からは、Ｃキーで暗号化されたデータと、Ｃキーが出力される。このＣキーは、Ｃキー取り込み回路１５５に送られ、Ｃキーで暗号化されたデータは、Ｃキー復号回路１５６に送られる。Ｃキー復号回路１５６で、Ｃキーによる解読が行なわれ、データが復号される。この復号され

たデータがデータ出力端子ＤＡＴＡ＿ＯＵＴから出力される。また、Ｃキーがキー出力端子ＫＥＹ＿ＯＵＴから出力される。

【００６４】

このようにコンテンツのデータをＣキーで暗号化しておくと、コンテンツのデータを利用するときには、必ず、これを解読するためのＣキーが必要になる。Ｃキーを有しているユーザ側の機器でのみ、そのコンテンツを利用可能なことから、Ｃキーは、そのコンテンツを利用できる権利を表すキーとして用いることができる。

【００６５】

すなわち、１つの機器から他の機器にＣキーを送れば、コンテンツとそのコンテンツを利用する権利が送られたことになり、他のユーザ側の機器で、そのコンテンツが利用可能となる。このように１つの機器から他のユーザ側の機器にＣキーを送った後にその機器のＣキーを消去してしまうと、たとえ送り側の機器にコンテンツが残っていても、そのコンテンツは最早利用できない。これは、そのコンテンツを譲渡したという見方ができる。

【００６６】

また、正規のユーザが誤ってコンテンツを消してしまったり、コンテンツのダウンロードに失敗してしまうような場合がある。この場合でも、Ｃキーが残っていれば、そのコンテンツを再送してもらい、そのコンテンツを利用することができる。このように、Ｃキーを導入することにより、以下のように、コンテンツの移動や再送が行なえるようになる。また、Ｃキーを利用することにより、課金の設定を行なうことができる。

【００６７】

暗号化／復号化処理チップ１２１のキー出力端子ＫＥＹ＿ＯＵＴからのＣキーと、データの出力端子ＤＡＴＡ＿Ｔからの Ｃキーで暗号化されたデータを相手側の機器に転送し、転送が終わったら、Ｃキー取り込み回路１５５に保存されているＣキー及びストレージデバイス１２０に保存されているＣキーを消去することで、コンテンツの移動が行なわれる。このようにすると、相手側の機器でのみコンテンツの利用が可能となる。このとき、ストレージデバイス１２０に残ってい

一致するか否かが判断される（ステップＳ４）。受信されたＣキーと、ストレージデバイス１２０に保存されているＣキーとが一致している場合には、再送であるので、課金は行なわれない（ステップＳ２）。

【００７１】

ステップＳ３でストレージデバイス１２０にＣキーが保存されていないと判断された場合、又はステップＳ４で、受信されたＣキーとストレージデバイス１２０に保存されているＣキーとが一致していないと判断された場合には、Ｃキーの課金ランクが取得される（ステップＳ５）。そして、この課金ランクに応じて、課金処理が行なわれる（ステップＳ６）。

【００７２】

４．Ｔキーを使ったシステムについて

このように、Ｃキーを導入することで、コンテンツのデータの移動、再送が行なえるようになる。ところが、Ｃキーのみでは、相手側の機器にコンテンツの移動を行なう際に、Ｃキーが直接転送される。このとき、Ｃキーが外部に漏れて、コンテンツのデータの保護が図られなくなる可能性がある。そこで、データを転送時のコンテンツのデータの保護を図るために、Ｔキーが導入される。

【００７３】

図６は、Ｔキーを導入したシステムの一例を示すものである。図６において、データの送り側のユーザマシン２０２Ａは、ストレージデバイス２２０Ａ、暗号化／復号化処理チップ２２１Ａ、入力部２２２Ａ、ユーザインターフェース２２３Ａ、マシン処理マネージャ２２４Ａ、通信マネージャ２２５Ａ、カードリーダ／ライタ２２７Ａから構成される。カードリーダ／ライタ２２７Ａには、カード２２６Ａが装着される。

【００７４】

データの受信側のユーザマシン２０２Ｂは、ストレージデバイス２２０Ｂ、暗号化／復号化処理チップ２２１Ｂ、入力部２２２Ｂ、ユーザインターフェース２２３Ｂ、マシン処理マネージャ２２４Ｂ、通信マネージャ２２５Ｂ、カードリーダ／ライタ２２７Ｂから構成される。カードリーダ／ライタ２２７Ｂには、カード２２６Ｂが装着される。

るコンテンツのデータは、消去しなくても良い。なぜなら、ストレージデバイス１２０に残っているコンテンツのデータは、Ｃキーで暗号化されており、Ｃキーが消去されてしまえば、そのコンテンツのデータは利用できないからである。

【００６８】

ストレージデバイス１２０のコンテンツのデータを消去してしまった後でも、Ｃキーが保存されていれば、コンテンツの再送が行なえる。コンテンツの再送は、前述のコンテンツデータのダウンロードの場合と同様の処理で行なわれる。このとき、新規のダウンロードであるか否かをＣキーで判断し、新規の場合のみ、課金を行なうようにする。

【００６９】

Ｃキーを使うと、コンテンツに応じた課金が行なえる。例えば、無料のコンテンツに対してはＣキーを付加せず、有料のコンテンツにのみＣキーを付加する。そして、受信側では、送られてきたＣキーが新規のものであるか否かを判断し、新規のＣキーの場合のみ、課金を行なうようにする。このようにすると、Ｃキーから、有料のコンテンツか否かを判断することができ、有料のコンテンツの保護が図れる。また、上述のコンテンツの再送のような場合には、保存されているＣキーと、受信されたコンテンツを暗号化するためのＣキーとを比較し、この比較結果から、課金を行なうかどうかを判断することができる。更に、課金に関する情報（例えば、コンテンツのランク付け等）をコード化してＣキーに包含させておき、同じコンテンツに対して条件により料金を変更できるようにすることも可能である。

【００７０】

図５は、Ｃキーを使った課金処理を示すフローチャートである。ダウンロードの際に、Ｃキーが受信されたか否かが判断される（ステップＳ１）。Ｃキーが受信されなければ、無料のコンテンツであるとして、課金は行なわれない（ステップＳ２）。Ｃキーが受信されたら、ストレージデバイス１２０にＣキーが保存されているか否かが判断される（ステップＳ３）。コンテンツの再送のような場合には、ストレージデバイス１２０にＣキーが残されている。このような場合には、受信されたＣキーと、ストレージデバイス１２０に保存されているＣキーとが

する際には、データを送出する側のユーザマシン２０２Ａから相手側のユーザマシン２０２ＢにＭＩＤコードの転送要求が送られる。

【００８０】

相手側のユーザマシン２０２Ｂでは、ＭＩＤコードの転送要求を受け付けると、ユーザマシン２０２Ｂの暗号化／復号化処理チップ２２１ＢのＭＩＤホルダ２５２からＭＩＤコードを呼び出し、このＭＩＤコードをコード出力端子ＭＩＤ＿ＯＵＴから出力させる。そして、このＭＩＤコードは、ユーザマシン２０２Ｂから、ユーザマシン２０２Ａに送られる。

【００８１】

データを送出する側のユーザマシン２０２Ａでは、コード入力端子ＭＩＤ＿ＩＮから相手側のユーザマシン２０２ＢからのＭＩＤコードを受け付けると、このＭＩＤコードをＴキー生成回路２５８Ａにセットする。Ｔキー生成回路２５８Ａは、この相手側のユーザマシン２０２Ｂから送られてきたＭＩＤコードに基づいて、Ｔキーを生成する。このＴキーがＴキー暗号化回路２５７Ａにセットされる。

【００８２】

ユーザマシン２０２ＢからのＭＩＤコードを受け付け、Ｔキー暗号化回路２５７ＡにこのＭＩＤコードに基づくＴキーがセットされたら、ユーザマシン２０１ＡからユーザマシンＢへのコンテンツのデータ及びＣキーのの転送が開始される。

【００８３】

ユーザマシン２０２Ａのストレージデバイス２２０Ａには、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータと、Ｍキーで暗号化されたＣキーが蓄積されている。したがって、ユーザマシン２０２Ａからユーザマシン２０２Ｂにコンテンツのデータ及びＣキーを転送する際に、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータと、Ｍキーで暗号化されたＣキーが、ユーザマシン２０２Ａのストレージデバイス２２０Ａから、暗号化／復号化処理チップ２２１Ａのキー入力端子ＫＥＹ＿ＩＮ及びデータ入力端子ＤＡＴＡ＿ＩＮに入力される。

【００８４】

Ｍキー復号化回路２５３Ａには、Ｍキーホルダ２５１ＡからＭキーが供給される。Ｍキー復号化回路２５３Ａで、Ｍキーホルダ２５１ＡからのＭキーによりＭキーの復号が行なわれる。このＭキー復号回路２５３Ａからは、Ｃキーと、Ｃキーで暗号化されたコンテンツのデータが出力される。Ｃキーは、Ｃキー取り込み回路２５５Ａに供給されると共に、Ｔキー暗号化回路２５７Ａに供給される。Ｃキーで暗号化されたコンテンツのデータは、Ｃキー復号化回路２５６Ａに供給されると共に、Ｔキー暗号化回路２５７Ａに供給される。

【００８５】

Ｃキー復号化回路２５６Ａで、Ｃキーの復号化処理が行なわれ、コンテンツのデータが復号される。復号されたデータは、データ出力端子ＤＡＴＡ＿ＯＵＴから出力される。

【００８６】

Ｔキー暗号化回路２５７Ａには、Ｔキー生成回路２５８ＡからＴキーが供給される。Ｔキー生成回路２５８Ａには、ユーザマシン２０２ＢのＭＩＤコードに基づいて生成されたＴキーが設定されている。Ｍキー復号回路２５３ＡからのＣキー及びＣキーで暗号化されたコンテンツのデータは、Ｔキー暗号化回路２５７Ａで、相手側のユーザマシン２０２ＢのＭＩＤコードに基づいて生成されたＴキーで暗号化される。したがって、Ｔキー暗号化回路２５７Ａからは、Ｔキーで暗号化されたＣキーと、Ｃキーで暗号化され更にＴキーで暗号化されたコンテンツのデータが出力される。

【００８７】

このＴキーで暗号化されたＣキーと、Ｃキーで暗号化され更にＴキーで暗号化されたコンテンツのデータは、キー出力端子ＴＫＥＹ＿ＯＵＴ及びデータ出力端子ＴＤＡＴＡ＿ＯＵＴから出力され、相手側のユーザマシン２０２Ｂに送られ、相手側のユーザマシン２０２Ｂの暗号化／復号化処理チップ２２１Ｂのキー入力端子ＲＣＫＥＹ＿ＩＮ及びデータ入力端子ＲＤＡＴＡ＿ＩＮに入力され、そして、Ｔキー復号化回路２６０Ｂに供給される。

【００８８】

Ｔキー復号化回路２６０Ｂには、Ｔキー生成回路２５９Ｂから、Ｔキーが与えられる。このＴキーは、ＭＩＤホルダ２５２ＢからのＭＩＤコードに基づいて生成されている。

【００８９】

送り側のユーザマシン２０２Ａでは、ユーザマシン２０２ＢからのＭＩＤコードを受信し、Ｔキー生成回路２５８Ａで、このＭＩＤコードに基づいて、Ｔキーを生成している。受信側のＴキー復号化回路２６０Ｂでは、ＭＩＤコードホルダ２５２ＢからのＭＩＤコードに基づいてＴキーを生成している。Ｔキー生成回路２５８Ａと２５９Ｂには、共に、同一ののＭＩＤコードが送られている。したがって、ユーザマシン２０２Ａから送られてきたコンテンツのデータ及びＣキーは、ユーザマシン２０２ＢのＴキー復号回路２６０Ｂで復号することができる。

【００９０】

Ｔキー復号化回路２６０Ｂからは、Ｃキーと、Ｃキーで暗号化されたコンテンツのデータが出力される。このＣキーと、Ｃキーで暗号化されたコンテンツのデータは、Ｍキー暗号化回路２６１Ｂに供給される。

【００９１】

Ｍキー暗号化回路２６１Ｂには、Ｍキーホルダ２５１Ｂから、機器固有のＭキーが与えられる。このＭキーにより、Ｃキーと、Ｃキーで暗号化されたコンテンツのデータは、暗号化される。したがって、Ｍキー暗号化回路２６１Ｂからは、Ｍキーで暗号化されたＣキーと、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータが出力される。このＭキーで暗号化されたＣキーと、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータは、キー出力端子ＲＫＥＹ＿ＯＵＴ及びデータ出力端子ＲＤＡＴＡ＿ＯＵＴから出力され、ユーザマシン２０２Ｂのストレージデバイス２２０Ｂに保存される。

【００９２】

このように、Ｔキーを用いると、ユーサマシン２０２Ａからユーザマシン２０２Ｂにデータを転送する際に、ユーサマシン２０２Ａからユーザマシン２０２Ｂに送られるＣキー及びＣキーで暗号化されたコンテンツのデータは、更にＴキー

で暗号化される。このため、外部に暗号化キーが漏れることがなく、コンテンツのデータの保護が図れる。

【００９３】

５．ＤＡコードを用いてシステム

このように、Ｔキーを導入すると、異なる機器間にデータを移動させる際のデータ保護を図ることができる。しかしながら、Ｔキーを導入したとしても、同一の機器内でデータを移動することは可能である。このため、Ｃキーを同一機器内の別の場所に一時的に保存しておいてから、コンテンツのデータの移動を行ない、その後に、Ｃキーを元に戻すようなことを行なうと、コンテンツのデータが不正に複製されてしまう。

【００９４】

そこで、Ｃキーに、時間と共に動的に変化するコード（ＤＡコードと称する）を付加して、Ｃキーに時間的に変化する要素を持たせることが考えられる。

【００９５】

つまり、図９において、ユーザマシン３０２は、ストレージデバイス３２０、暗号化／復号化処理チップ３２１、入力部３２２、ユーザインターフェース３２３、マシン処理マネージャ３２４、通信マネージャ３２５、カードリーダ／ライタ３２７から構成される。カードリーダ／ライタ３２７には、カード３２６が装着される。

【００９６】

このような機器で、例えばストレージデバイス３２０からＣキーを読み出し、このＣキーをＣキー保存メモリ３３０に保存しておいてから、ストレージデバイス３２０のコンテンツのデータを他の機器に移動したとする。この場合、データの移動が終了すると、ストレージデバイス３２０のＣキーは消されるが、Ｃキー保存メモリ３３０にＣキーを退避させておけば、このＣキーは消去されない。その後、Ｃキー保存メモリ３３０からのＣキーをストレージデバイス３２０に戻せば、ストレージデバイス３２０にコンテンツのデータがあれば、このコンテンツのデータを復号できてしまう。また、ストレージデバイス３２０にコンテンツデータが無くても、Ｃキーがあれば、コンテンツデータの再送が要求できる。

【００９７】

そこで、図１０に示すように、Ｃキーに対して、時間と共に動的に変化するＤＡコードが付加される。このＤＡコードとしては、タイムコードや乱数が用いられる。このように、Ｃキーに対してＤＡコードを付加することにより、コンテンツの不正利用を防止することができる。

【００９８】

図１１は、ＤＡコードが付加されたＣキーを扱うための暗号化／復号化処理チップ３２１の構成を示すものである。図１１に示すように、暗号化／復号化処理チップ３２１には、Ｍキーホルダ３５１と、ＭＩＤホルダ３５２と、Ｍキー復号化回路３５３と、コントローラ３５４と、Ｃキー取り込み回路３５５と、Ｃキー復号化回路３５６と、Ｔキー暗号化回路３５７と、Ｔキー生成回路３５８、３５９と、Ｔキー復号化回路３６０と、Ｍキー暗号化回路３６１とが設けられると共に、ＤＡコード管理回路３６２とが設けられる。

【００９９】

ＤＡコード管理回路３６２は、Ｃキーに付加するＤＡコードの管理を行なうものである。すなわち、ＤＡコード管理回路３６２は、所定時間毎にストレージデバイス３２０からのＣキーを呼び出しを行なう。Ｃキーが呼び出されると、ＤＡコードのチェックを行い、ＤＡコードが正しければ、ＤＡコートの更新処理を行なう。

【０１００】

なお、ストレージデバイス３２０には、Ｍキーで暗号化されたＣキーが保存されている。したがって、このＭキーで暗号化されたＣキーは、先ず、キー入力端子ＫＥＹ＿ＩＮから、Ｍキー復号化回路３５３に送られて、復号される。Ｍキー復号化回路３５３から、Ｃキーが出力され、このＣキーは、ＤＡコード管理回路３６２に送られる。

【０１０１】

ＤＡコード管理回路３６２は、このＤＡコードを所定時間毎に検出して正しく更新されているＤＡコードが付加されているか否かを判断し、正しく更新されているＤＡコードなら、ＤＡコードの更新を行なう。そして、このＤＡコードを更

新したＣキーをＭキー暗号化回路３６１に送って暗号化して、再び、ストレージデバイス３２０に保存する。

【０１０２】

図１２は、ＤＡコード管理回路３６２の処理を示すフローチャートである。図１２において、所定時間経過したか否かが判断され（ステップＳ１１）、所定時間経過したら、Ｃキーが呼び出され、Ｃキーに付加されているＤＡコードが検出される（ステップＳ１２）。そして、このＤＡコードが正しく更新されているＤＡコードであるか否かが判断される（ステップＳ１３）。ＤＡコードが正しく更新されているか否かは、チップ３１内に保持しているＤＡコードとストレージデバイス３２０から読み出されたＤＡコードが一致しているか否かにより判断できる。ステップＳ１３で正しく更新されているＤＡコードであると判断されると、このＤＡコードが次のＤＡコードに更新され、そして、この更新されたＤＡコードが付加されたＣキーは、再び、ストレージデバイス３２０に戻される（ステップＳ１４）。

【０１０３】

ステップＳ１３で、検出されたＤＡコードが正しく更新されているＤＡコードではないと判断されたら、Ｃキーを消去し、又は、Ｃキーに不正利用を示すコードを付加して、そのコンテンツの利用が禁止される（ステップＳ１５）。

【０１０４】

このように、ストレージデバイスのＣキーが正常に扱われている場合には、ＤＡコード管理回路３６２で、Ｃキーに付加されるＤＡコードが絶えず更新され、更新されたＤＡコードが付加されたＣキーがストレージデバイス３２０に保存される。

【０１０５】

例えば、Ｃキーを図９におけるＣキー保存メモリ３３０に保存しておいたような場合には、ＣキーのＤＡコードが更新されないので、ＤＡコード管理回路３６２で、ＤＡコートが正しくないと判断される。これにより、コンテンツのデータの不正利用が防止できる。

【０１０６】

なお、このような動的に変化するＤＡコードを使うと、ある期間再生を禁止／許可することができるようになる。これを利用すると、コンテンツを所定の期間貸し出したり、コンテンツの利用に試用期間を設定したりすることができる。

【０１０７】

図１３は、所定期間だけ再生可能に設定する場合の処理を示すフローチャートである。なお、この場合、ＤＡコードとして、タイムコードが用いられる。また、このＣキーに、更に、期限情報が付加される。

【０１０８】

図１３において、所定時間経過したか否かが判断され（ステップＳ２１）、所定時間経過したら、ストレージデバイスに保存されているＣキーが呼び出される。そして、このＣキーに付加されているＤＡコードが検出される（ステップＳ２２）。そして、ＤＡコードが正しく更新されているか否かが判断される（ステップＳ２３）。ステップＳ２３で正しく更新されているＤＡコードであると判断されると、このＤＡコードが次のＤＡコードに更新される（ステップＳ２４）。そして、この更新されたＤＡコードと期限情報とが比較され、期限超過か否かが判断される（ステップＳ２５）。期限超過でなければ、この更新されたＤＡコードが付加されたＣキーがストレージデバイスに戻され（ステップＳ２６）、ステップＳ２１リターンされる。

【０１０９】

ステップＳ２３で、ストレージデバイスから呼び出されたＤＡコードが正しく更新されているものではないと判断されたら、このＣキーが削除され、又は、不正使用を示すコードが付加されて、利用不可能とされる。（ステップＳ２６）。また、ステップＳ２５で、期間超過であると判断されると、ステップＳ２６に行き、Ｃキーが削除され、又は、不正使用を示すコードが付加されて、利用不可能とされる。

【０１１０】

このようにして、ＤＡコードを用いて、ある期間再生を禁止／許可したりすることができる。これにより、試用期間を設けて、データを再生させるようなこと

ができる。更に、一方のユーザマシンから他方のユーザマシンにコンテンツのデータを移動する場合に、一方のユーザマシンのＣキーをＤＡコードにより所定の期限まで再生禁止とし、他方のユーザマシンのＣキーをその期間のみ再生可能とすると、一方のマシンから他方のマシンに所定の期間だけコンテンツのデータを貸すような制御が行なえる。

【０１１１】

【発明の効果】

この発明によれば、コンテンツサーバに保存されるコンテンツは、Ｃキーで暗号化されている。このように、Ｃキーを設けることにより、コンテンツを移動したり、再送を要求したりできる。また、送られてきたＣキーと同一のＣキーがストレージデバイスに保存さているか否かを判断することにより、再送か否かを判断して、適切な課金を行なったり、Ｃキーにランクを付けてコンテンツ毎に料金を変えて課金を行なうようなことができる。

【０１１２】

また、この発明によれば、Ｃキーに、時間と共に動的に変化するＤＡコードが付加される。このようなＤＡコードを付加することで、Ｃキーを退避させておいて、コンテンツを不正利用するようなことが防止できる。また、この時間と共に動的に変化するＤＡコードを利用して、コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借するようなことが行なえる。

【図面の簡単な説明】

【図１】

この発明が適用できるデータ配信システムにおけるＭキーを用いたシステムの説明に用いるブロック図である。

【図２】

この発明が適用できるデータ配信システムにおけるＭキーを用いたシステムの暗号化／復号化処理チップの説明に用いるブロック図である。

【図３】

この発明が適用できるデータ配信システムにおけるＣキーを用いたシステムの説明に用いるブロック図である。

【図４】

この発明が適用できるデータ配信システムにおけるＣキーを用いたシステムの暗号化／復号化処理チップの説明に用いるブロック図である。

【図５】

この発明が適用できるデータ配信システムにおけるＣキーを用いたシステムの説明に用いるフローチャートである。

【図６】

この発明が適用できるデータ配信システムにおけるＴキーを用いたシステムの説明に用いるブロック図である。

【図７】

この発明が適用できるデータ配信システムにおけるＴキーを用いたシステムの暗号化／復号化処理チップの説明に用いるブロック図である。

【図８】

この発明が適用できるデータ配信システムにおけるＴキーを用いたシステムにおける暗号化／復号化処理チップの説明に用いるブロック図である。

【図９】

この発明が適用できるデータ配信システムにおけるＤＡコードを用いたシステムの説明に用いるブロック図である。

【図１０】

ＤＡコードの説明に用いる略線図である。

【図１１】

この発明が適用できるデータ配信システムにおけるＤＡコードを用いてシステムの暗号化／復号化処理チップの説明に用いるブロック図ある。

【図１２】

この発明が適用できるデータ配信システムにおけるＤＡコードを用いたシステムの説明に用いるフローチャートである。

【図１３】

この発明が適用できるデータ配信システムにおけるＤＡコードを用いたシステムの説明に用いるフローチャートである。

【００７５】

Ｔキーを導入したシステムでは、暗号化／復号化処理チップ２２１Ａ及び２２１Ｂとして、図７に示すようなものが用いられる。図７に示すように、暗号化／復号化処理チップ２２１Ａ及び２２１Ｂには、Ｍキーホルダ２５１と、ＭＩＤコードホルダ２５２と、Ｍキー復号化回路２５３と、コントローラ２５４と、Ｃキー取り込み回路２５５と、Ｃキー復号化回路２５６とが設けられると共に、Ｔキー暗号化回路２５７と、Ｔキー生成回路２５８、２５９と、Ｔキー復号化回路２６０と、Ｍキー暗号化回路２６１とが設けられる。

【００７６】

Ｍキーホルダ２５１、ＭＩＤコードホルダ２５２、Ｍキー復号化回路２５３、コントローラ２５４の動作は、前述までのシステムにおける暗号化／復号化処理チップ２１、１２１と同様であり、Ｍキーホルダ２５１には、各機器固有の暗号化情報であるＭキーが工場出荷時に記憶され、ＭＩＤコードホルダ２５２には、各機器固有の識別情報であるＭＩＤコードが工場出荷時に記憶され、コントローラ２５４は、暗号化／復号化処理チップ２２１Ａ、２２１Ｂの動作を制御している。また、Ｃキー取り込み回路２５５は、Ｍキーの解読により復号されたＣキーを保持し、Ｃキー復号回路２５６は、Ｃキーの復号化処理を行なう。

【００７７】

Ｔキー暗号化回路２５７は、Ｔキー生成回路２５８からのＴキーにより、転送するデータをＴキーで暗号化するものである。Ｔキー復号回路２６０は、Ｔキー生成回路２５９からのＴキーにより、転送されてきたデータを復号するものである。なお、Ｔキー生成回路２５８及び２５９は、ＭＩＤコードに基づいてＴキーを生成するものであり、そのアルゴリズムは同一である。

【００７８】

図６において、ユーザマシン２０２Ａからユーザマシン２０２Ｂに、コンテンツのデータを移動するとする。図８は、このときの暗号化／復号化処理チップ２２１Ａ、２２１Ｂの動作を説明するためのものである。

【００７９】

ユーザマシン２０２Ａからユーザマシン２０２Ｂにコンテンツのデータを移動

【図１４】

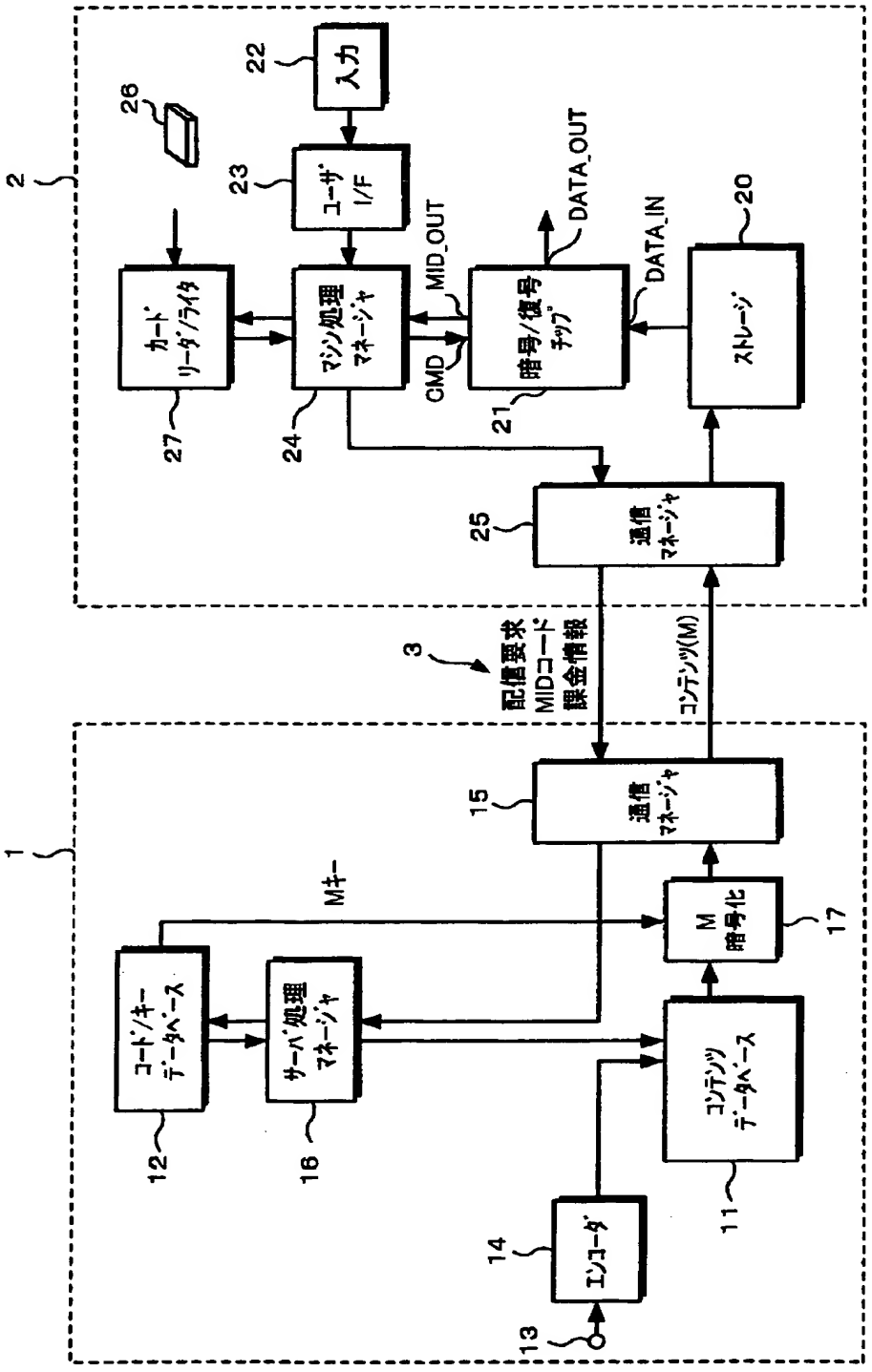
従来のデータ配信システムの一例のブロック図である。

【符号の説明】

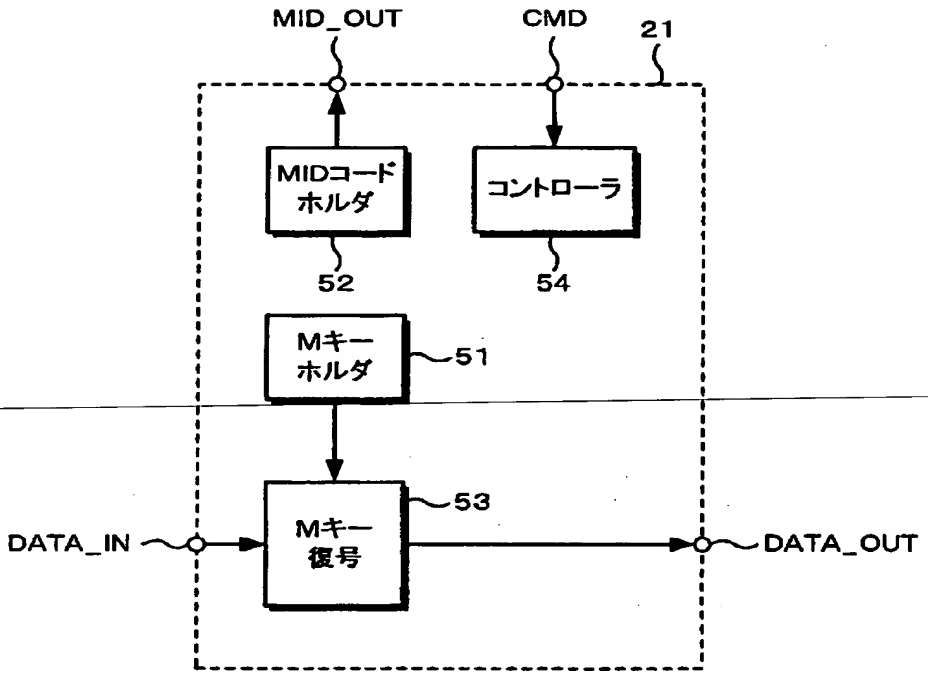
１、１０１・・・コンテンツサーバ、２、１０２、２０２Ａ、２０２Ｂ、３０２・・・ユーザマシン、２０、１２０、２２０Ａ、２２０Ｂ、３２０・・・ストレージデバイス、２１、１２１、２２１Ａ、２２１Ｂ、３２１・・・暗号化／復号化処理チップ

【書類名】　図面

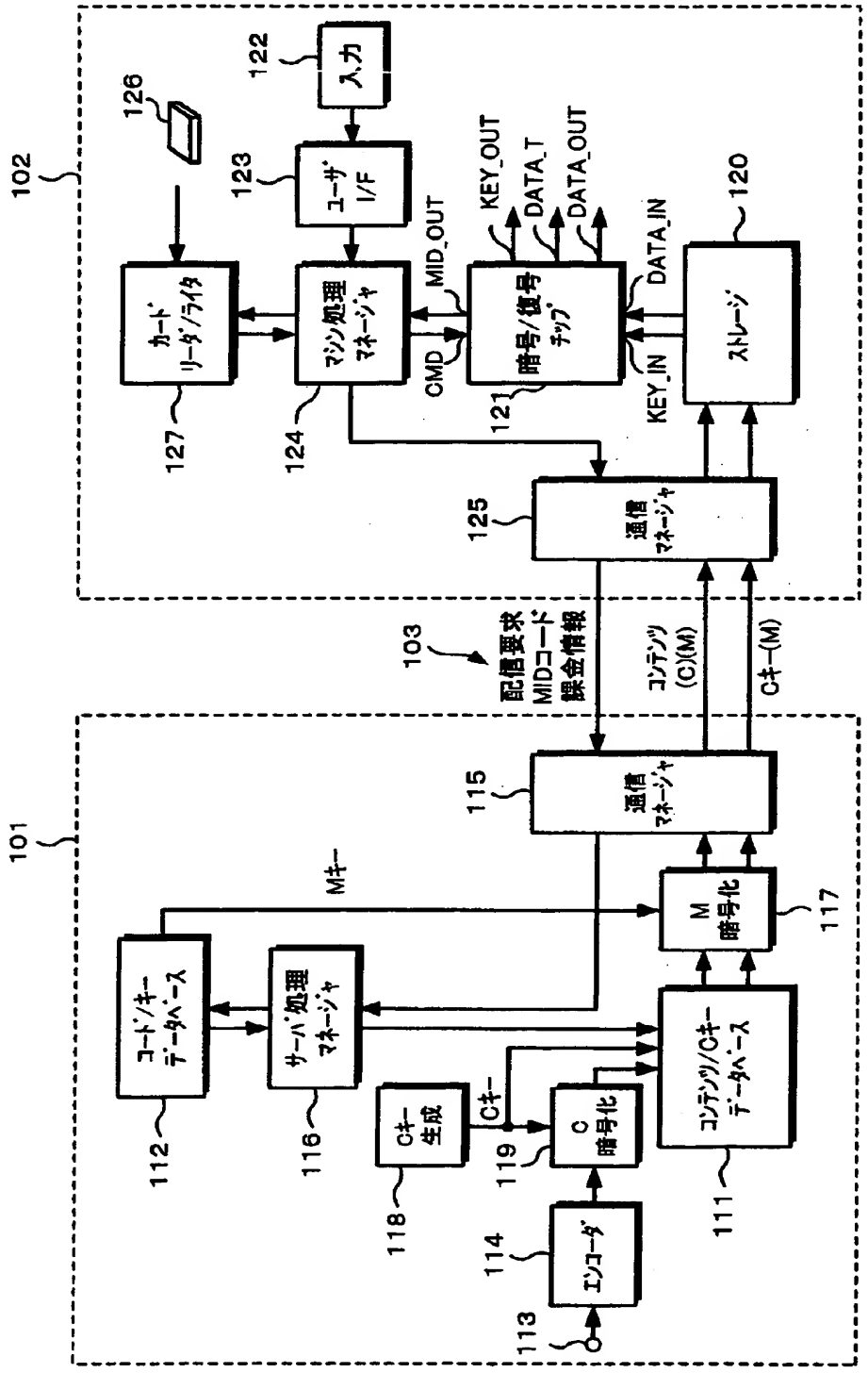
【図１】


2
22
入力
26
23
ユーザ I/F
カード リーダ/ライタ
マシン処理 マネージャ
MID_OUT
CMD
暗号/復号 チップ
DATA_OUT
DATA_IN
ストレージ
20
27
24
21
25
通信 マネージャ
3
配信要求
MIDコード
課金情報
コンテンツ(M)
1
15
通信 マネージャ
Mキー
M 暗号化
17
コード/キー データベース
サーバ処理 マネージャ
コンテンツ データベース
12
16
11
14
エンコーダ
13

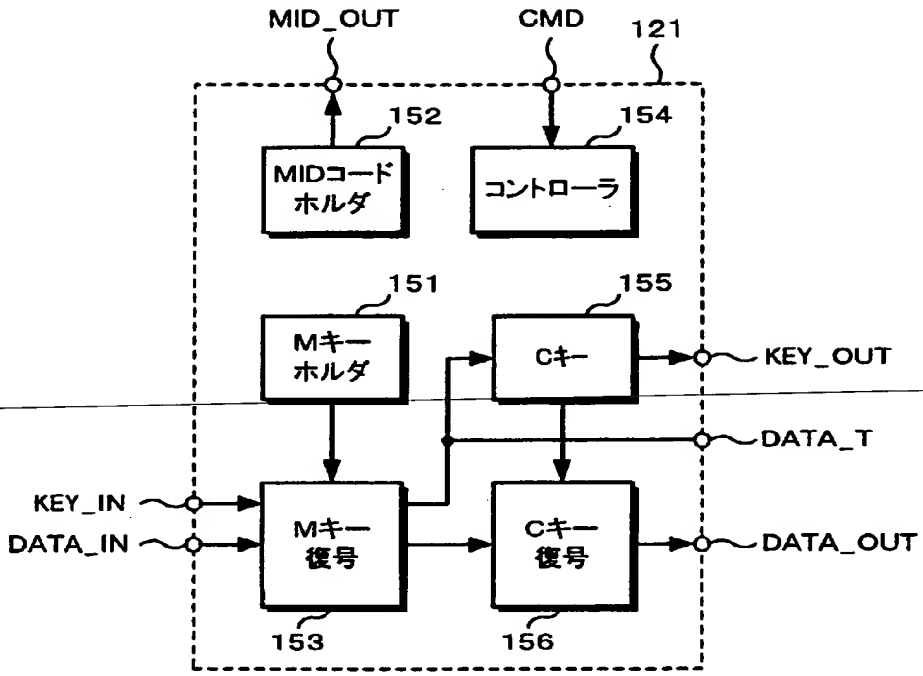
【図２】


MID_OUT
CMD
21
MIDコード
ホルダ
コントローラ
52
54
Mキー
ホルダ
51
53
DATA_IN
Mキー
復号
DATA_OUT

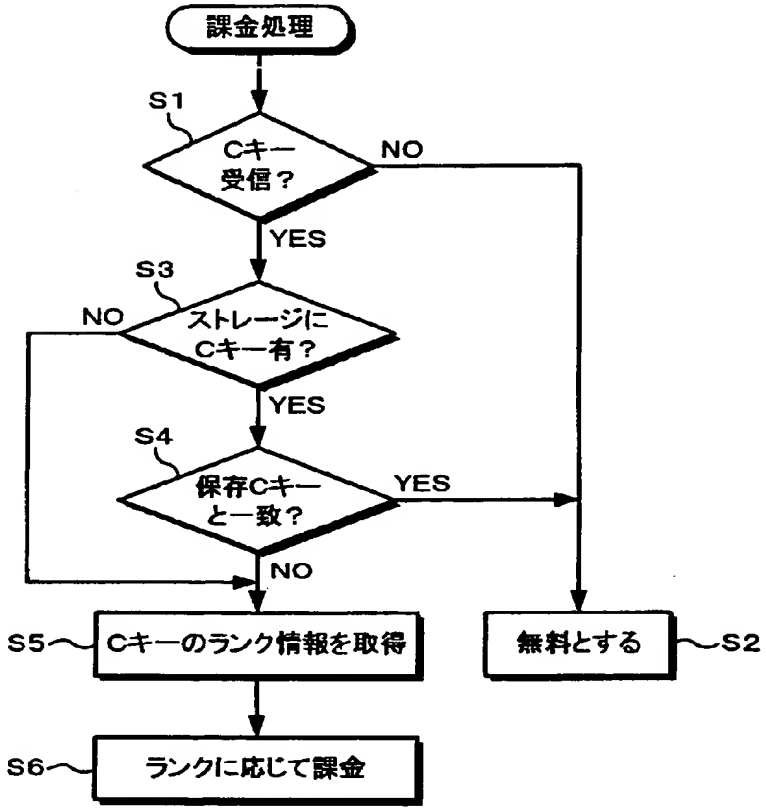
【図３】


102
126
122
入力
123
ユーザ I/F
127
カード リーダ/ライタ
124
マシン処理 マネージャ
MID_OUT
CMD
121
暗号/復号 チップ
KEY_OUT
DATA_T
DATA_OUT
DATA_IN
KEY_IN
120
ストレージ
125
通信 マネージャ
103
配信要求 MIDコード 課金情報
コンテンツ (C)(M)
Cキー(M)
101
115
通信 マネージャ
Mキー
M 暗号化
117
112
コード/キー データベース
116
サーバ処理 マネージャ
118
C キー 生成
Cキー
119
C 暗号化
111
コンテンツ/Cキー データベース
114
エンコーダ
113

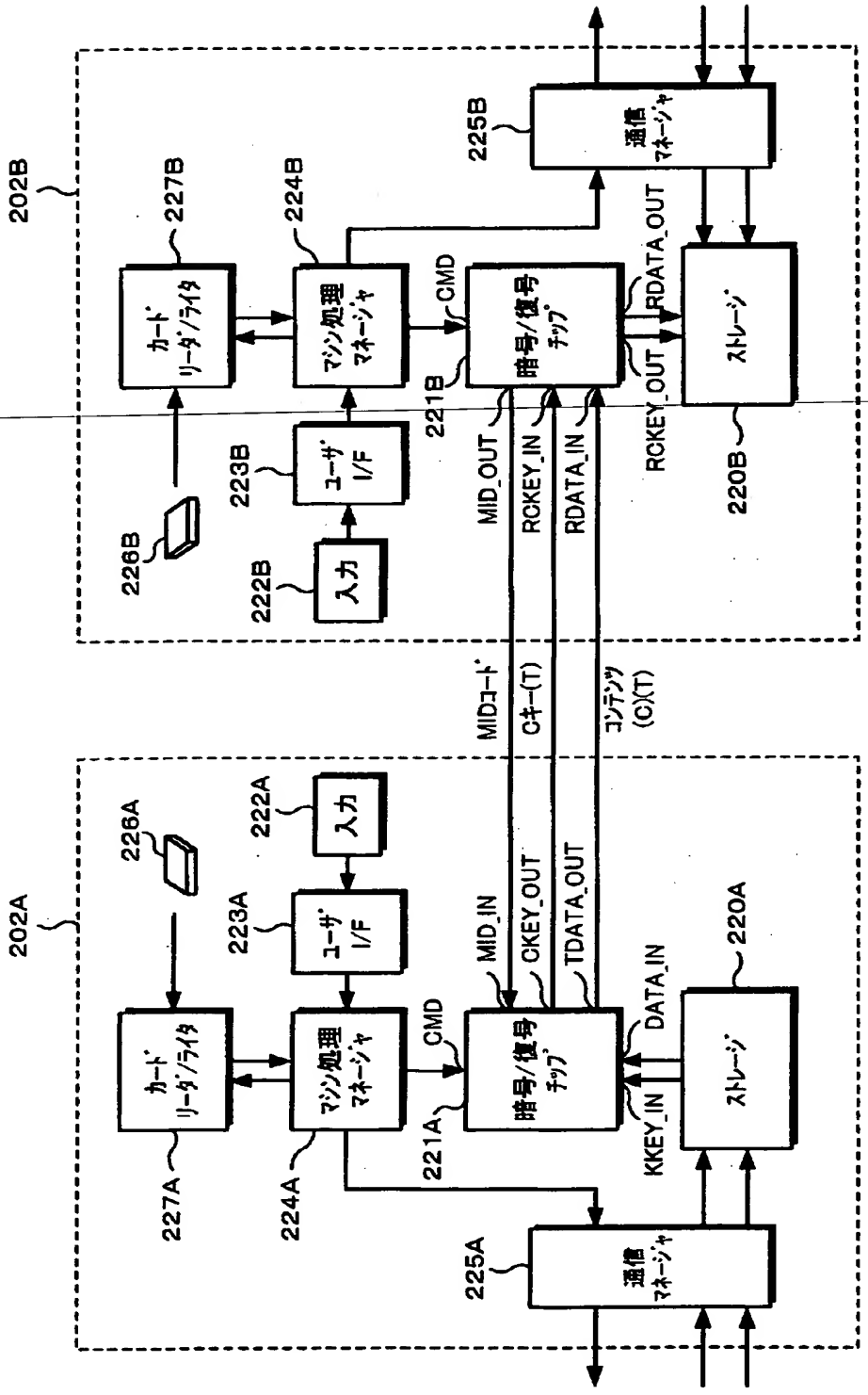
【図４】


MID_OUT
CMD
121
152
154
MIDコード
ホルダ
コントローラ
151
155
Mキー
ホルダ
Cキー
KEY_OUT
DATA_T
KEY_IN
DATA_IN
Mキー
復号
Cキー
復号
DATA_OUT
153
156

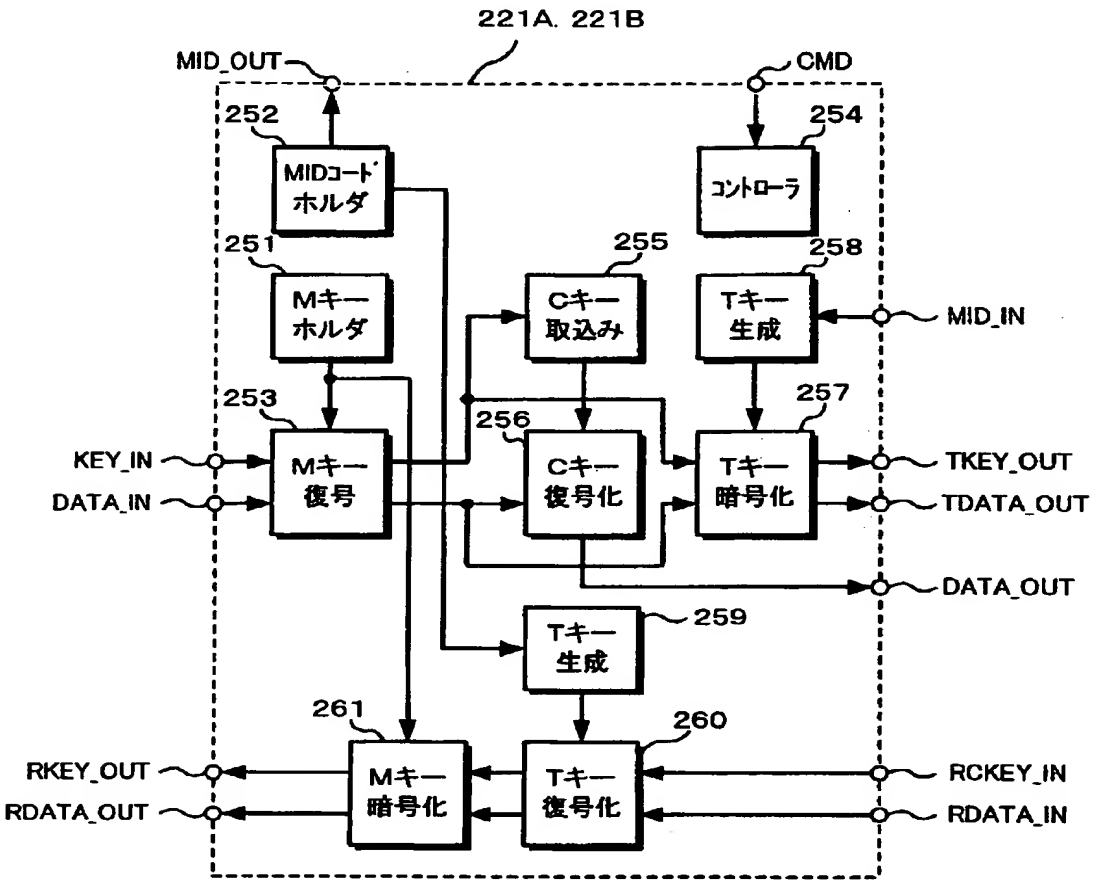
【図５】


課金処理
S1
Cキー
受信？
NO
YES
S3
NO
ストレージに
Cキー有？
YES
S4
保存Cキー
と一致？
YES
NO
S5
Cキーのランク情報を取得
無料とする
S2
S6
ランクに応じて課金

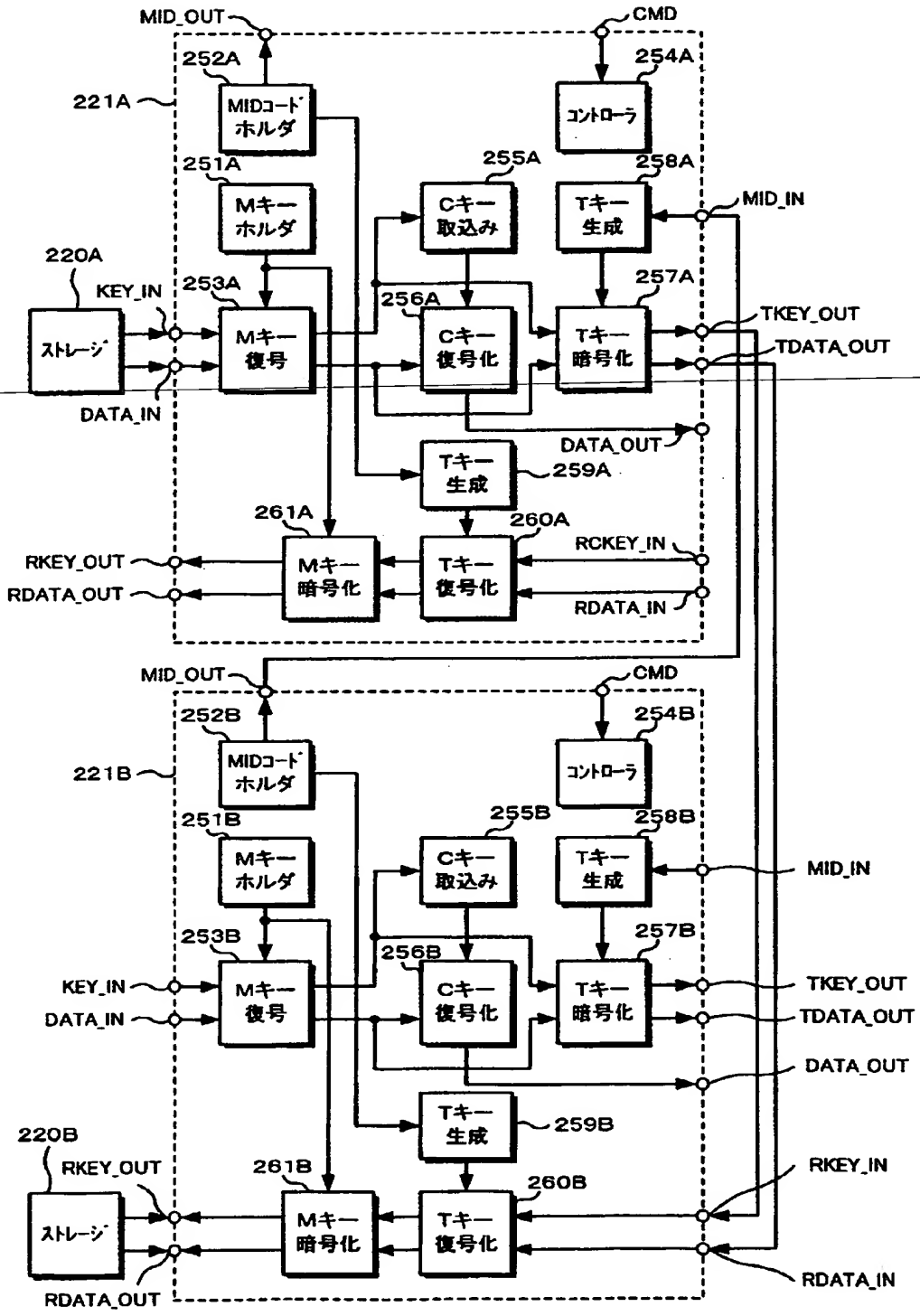
【図６】


202B
227B
カード
リーダ/ライタ
224B
マシン処理
マネージャ
CMD
暗号/復号
チップ
225B
通信
マネージャ
RDATA_OUT
ストレージ
RKEY_OUT
220B
221B
MID_OUT
RKEY_IN
RDATA_IN
223B
ユーザ
I/F
222B
入力
226B
MIDコード
Cキー(T)
コンテンツ
(C)(T)
202A
226A
222A
入力
223A
ユーザ
I/F
MID_IN
CKEY_OUT
TDATA_OUT
220A
カード
リーダ/ライタ
マシン処理
マネージャ
CMD
暗号/復号
チップ
DATA_IN
ストレージ
227A
224A
221A
KKEY_IN
225A
通信
マネージャ

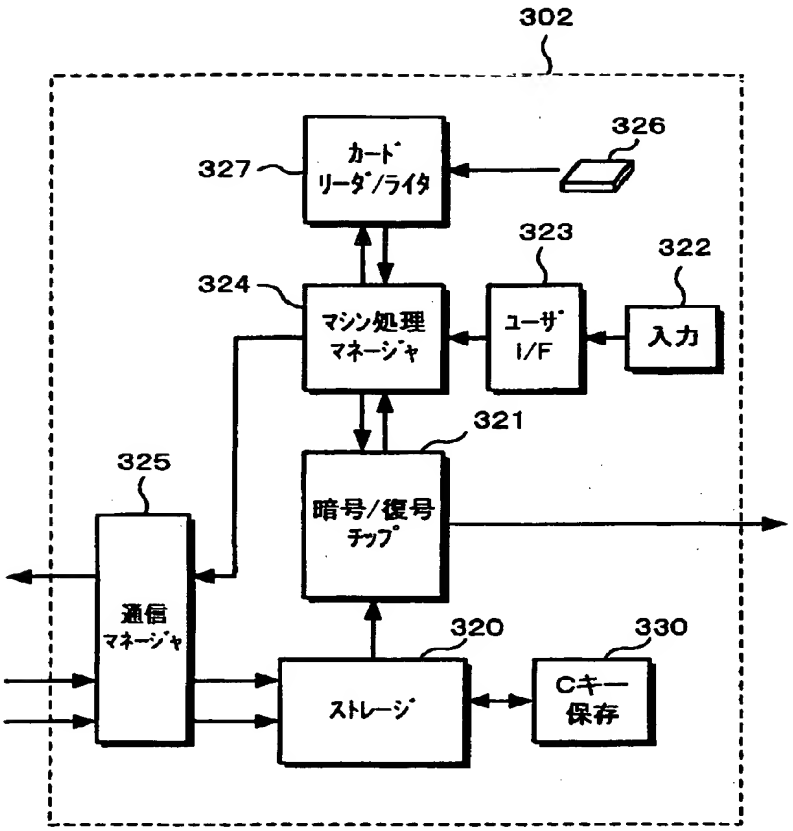
【図７】


221A. 221B
MID_OUT
CMD
252
MIDコード
ホルダ
254
コントローラ
251
Mキー
ホルダ
255
Cキー
取込み
258
Tキー
生成
MID_IN
253
256
257
KEY_IN
DATA_IN
Mキー
復号
Cキー
復号化
Tキー
暗号化
TKEY_OUT
TDATA_OUT
DATA_OUT
259
Tキー
生成
261
260
RKEY_OUT
RDATA_OUT
Mキー
暗号化
Tキー
復号化
RCKEY_IN
RDATA_IN

【図８】


MID_OUT
CMD
252A
254A
221A
MIDコードホルダ
コントローラ
251A
255A
258A
Mキーホルダ
Cキー取込み
Tキー生成
MID_IN
220A
KEY_IN
253A
256A
257A
ストレージ
Mキー復号
Cキー復号化
Tキー暗号化
TKEY_OUT
TDATA_OUT
DATA_IN
DATA_OUT
Tキー生成
259A
261A
260A
RCKEY_IN
RKEY_OUT
RDATA_OUT
Mキー暗号化
Tキー復号化
RDATA_IN
MID_OUT
CMD
252B
254B
221B
MIDコードホルダ
コントローラ
251B
255B
258B
Mキーホルダ
Cキー取込み
Tキー生成
MID_IN
253B
256B
257B
KEY_IN
DATA_IN
Mキー復号
Cキー復号化
Tキー暗号化
TKEY_OUT
TDATA_OUT
DATA_OUT
Tキー生成
259B
220B
RKEY_OUT
261B
260B
RKEY_IN
ストレージ
Mキー暗号化
Tキー復号化
RDATA_OUT
RDATA_IN

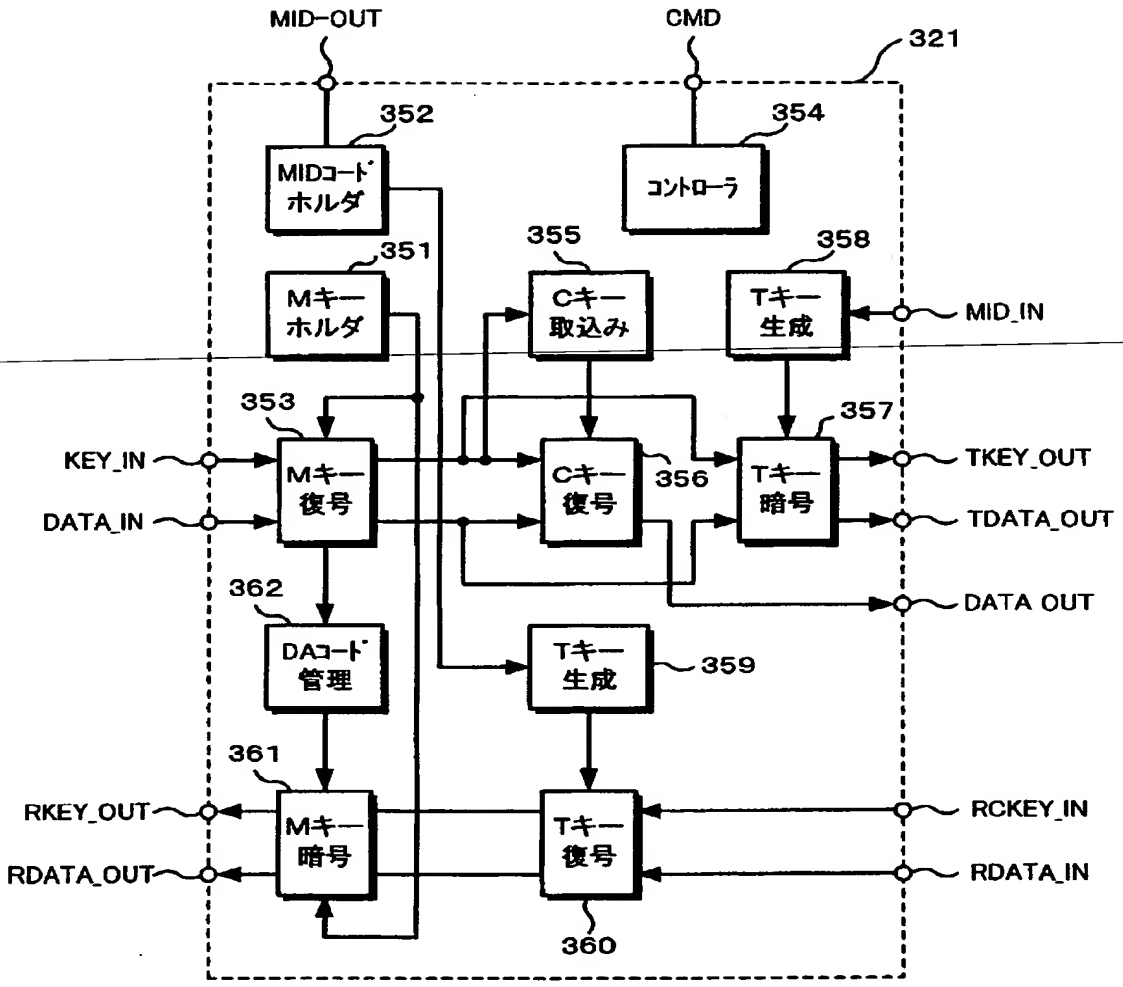
【図９】


302
326
327
カード
リーダ/ライタ
323
322
324
マシン処理
マネージャ
ユーザ
I/F
入力
321
325
暗号/復号
チップ
通信
マネージャ
320
330
ストレージ
Cキー
保存

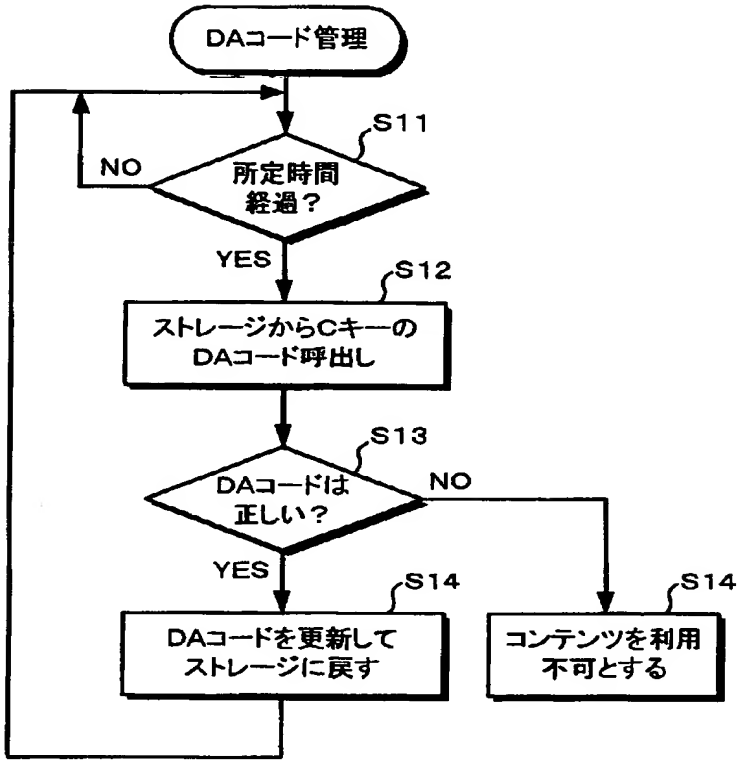
【図１０】


Cキー
DAコード

【図１１】

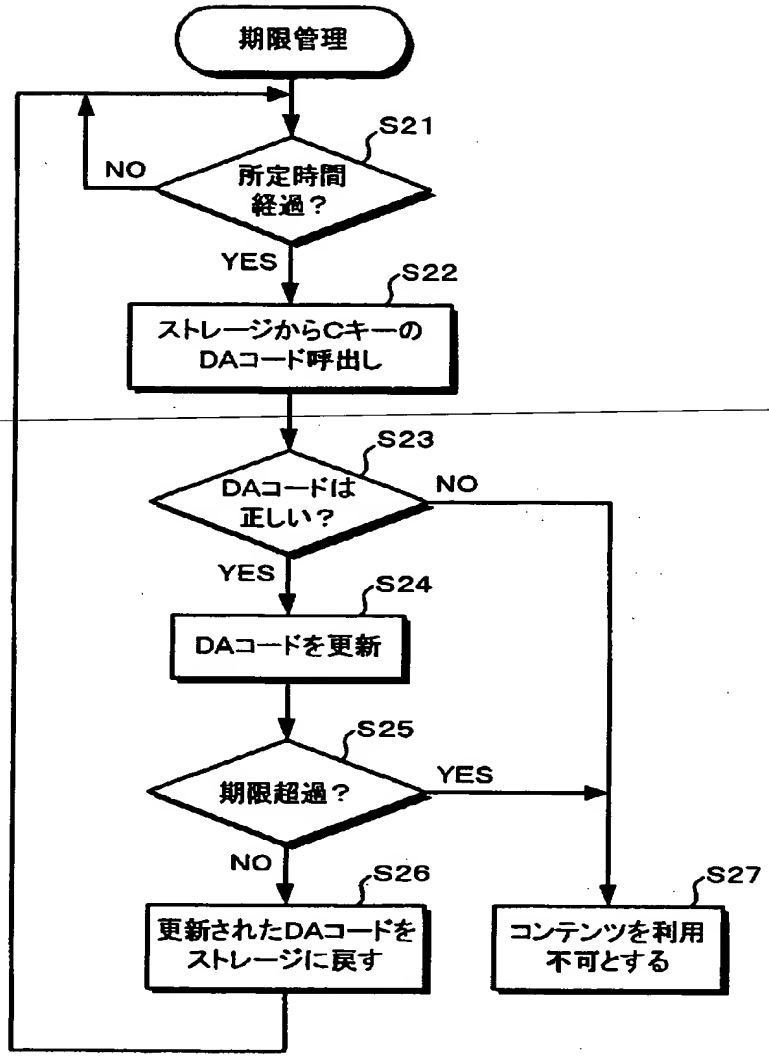

MID-OUT
CMD
321
352
354
MIDコード
ホルダ
コントローラ
355
358
351
Mキー
ホルダ
Cキー
取込み
Tキー
生成
MID_IN
353
357
KEY_IN
Mキー
復号
Cキー
復号
356
Tキー
暗号
TKEY_OUT
DATA_IN
TDATA_OUT
DATA OUT
362
DAコード
管理
Tキー
生成
359
361
RKEY_OUT
Mキー
暗号
Tキー
復号
RCKEY_IN
RDATA_OUT
RDATA_IN
360

【図１２】

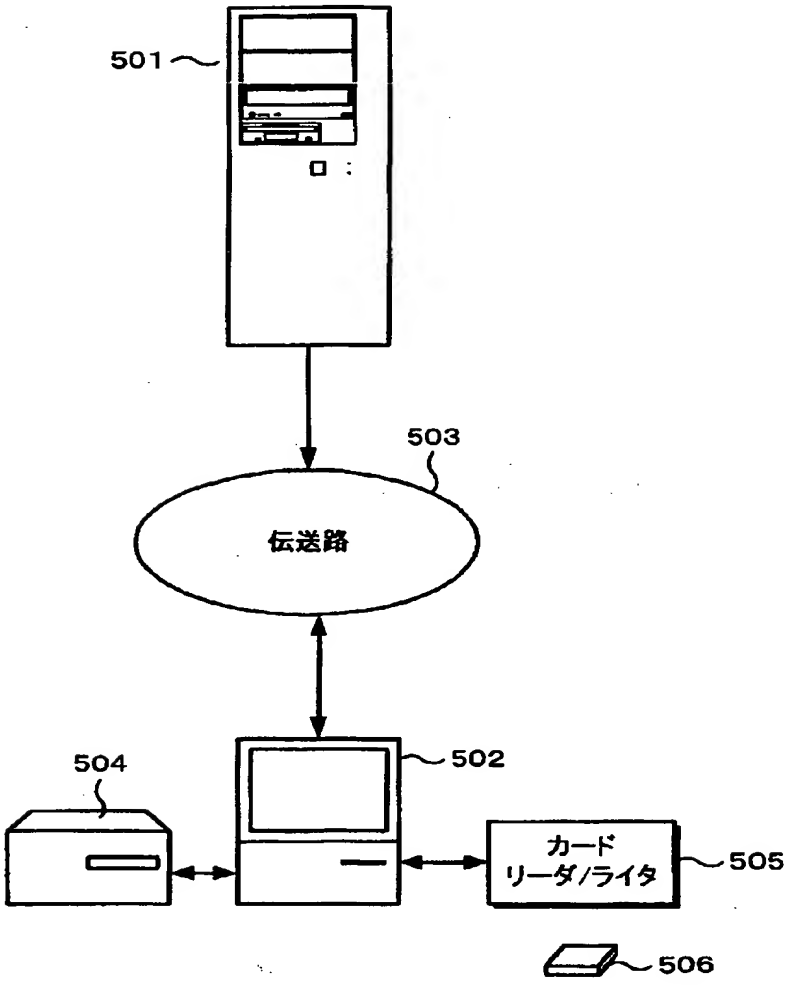


出証特平１１－３０１９３８２

【図１３】


期限管理
S21
NO
所定時間
経過？
YES
S22
ストレージからCキーの
DAコード呼出し
S23
DAコードは
正しい？
NO
YES
S24
DAコードを更新
S25
期限超過？
YES
NO
S26
更新されたDAコードを
ストレージに戻す
S27
コンテンツを利用
不可とする

【図１４】



THIS PAGE BLANK (USPTO)